

FIG. 1

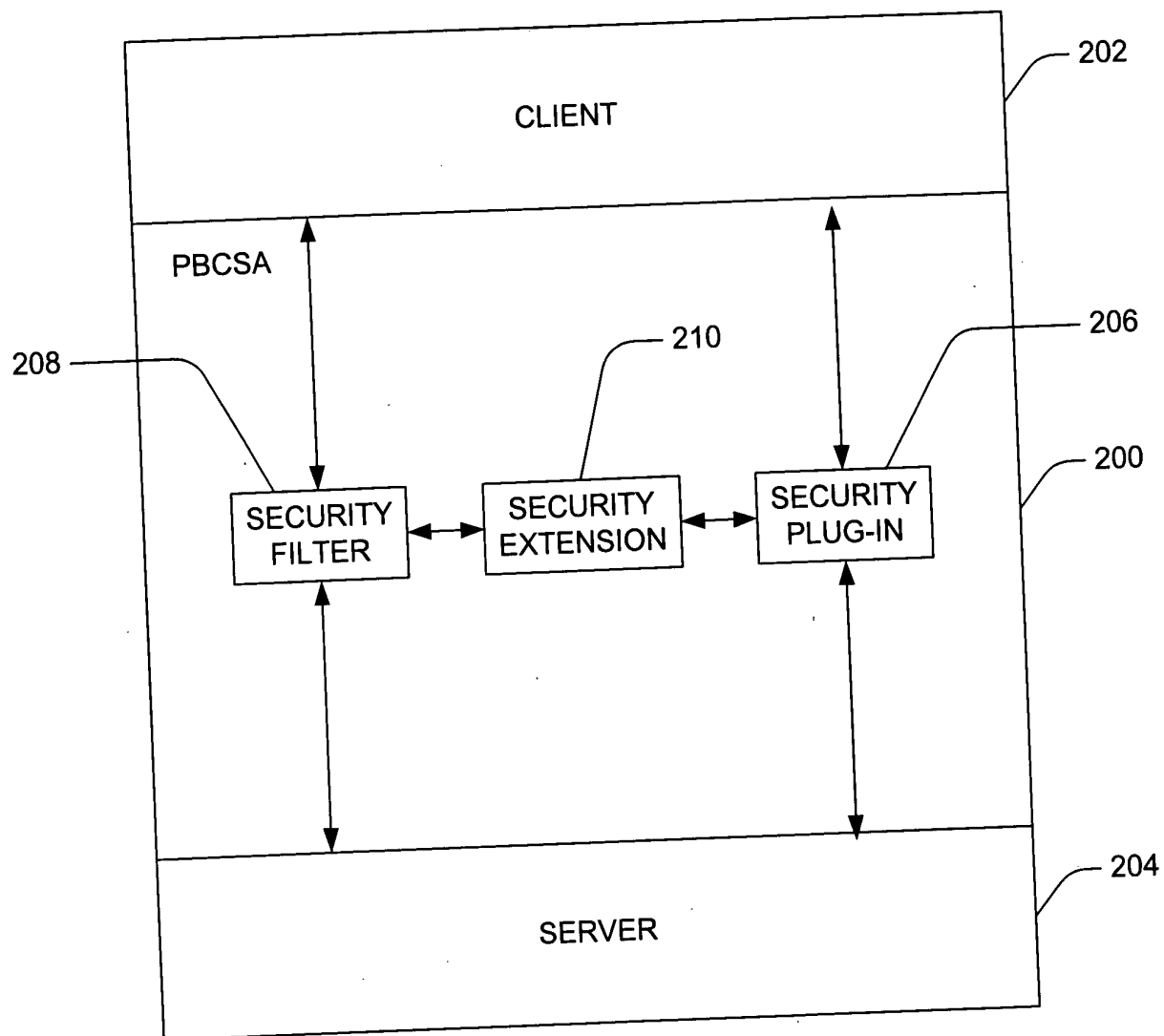


FIG. 2

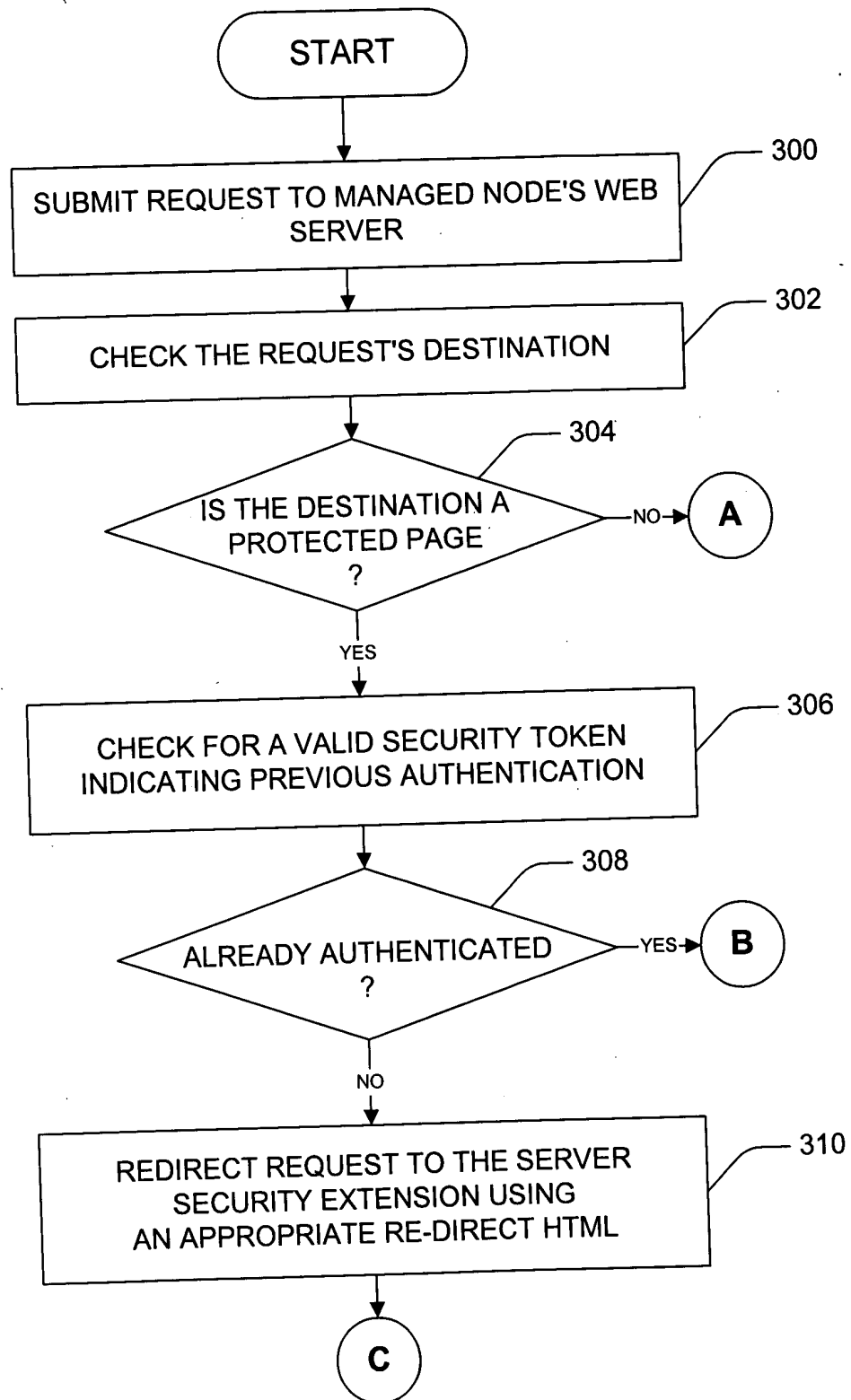


FIG. 3A

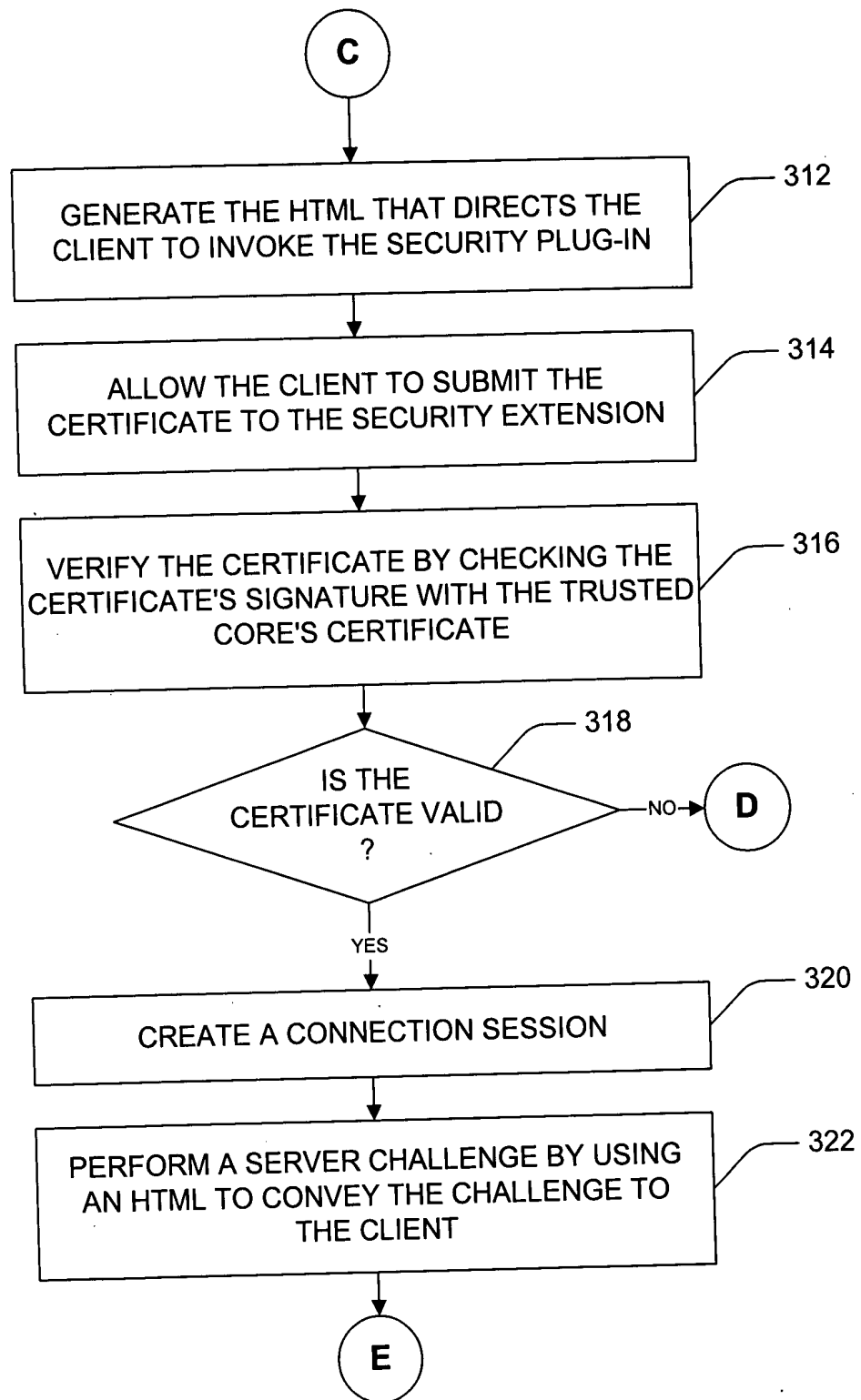


FIG. 3B

```
graph TD
    E((E)) --> 324[324 DIRECT THE CLIENT TO INVOKE THE SECURITY PLUG-IN TO GENERATE THE CLIENT RESPONSE TO THE SERVER CHALLENGE]
    324 --> 326[326 SAVE THE SECURITY TOKEN AS A NAMED COOKIE]
    326 --> 328[328 RE-SUBMIT THE ORIGINAL REQUEST URL WITH THE QUERY STRING TO THE SERVER]
    328 --> 330[330 CONFIRM AUTHENTICATION USING THE SECURITY TOKEN CONTAINED IN THE COOKIE]
    330 --> 332{332 IS THE CLIENT AUTHORIZED TO ACCESS THE PAGE?}
    332 -- YES --> 334[334 ALLOW ACCESS TO THE REQUESTED PAGE]
    332 -- NO --> B((B))
    334 --> A((A))
    B --> A
    A --> D((D))
    D --> END([END])
```

FIG. 3C

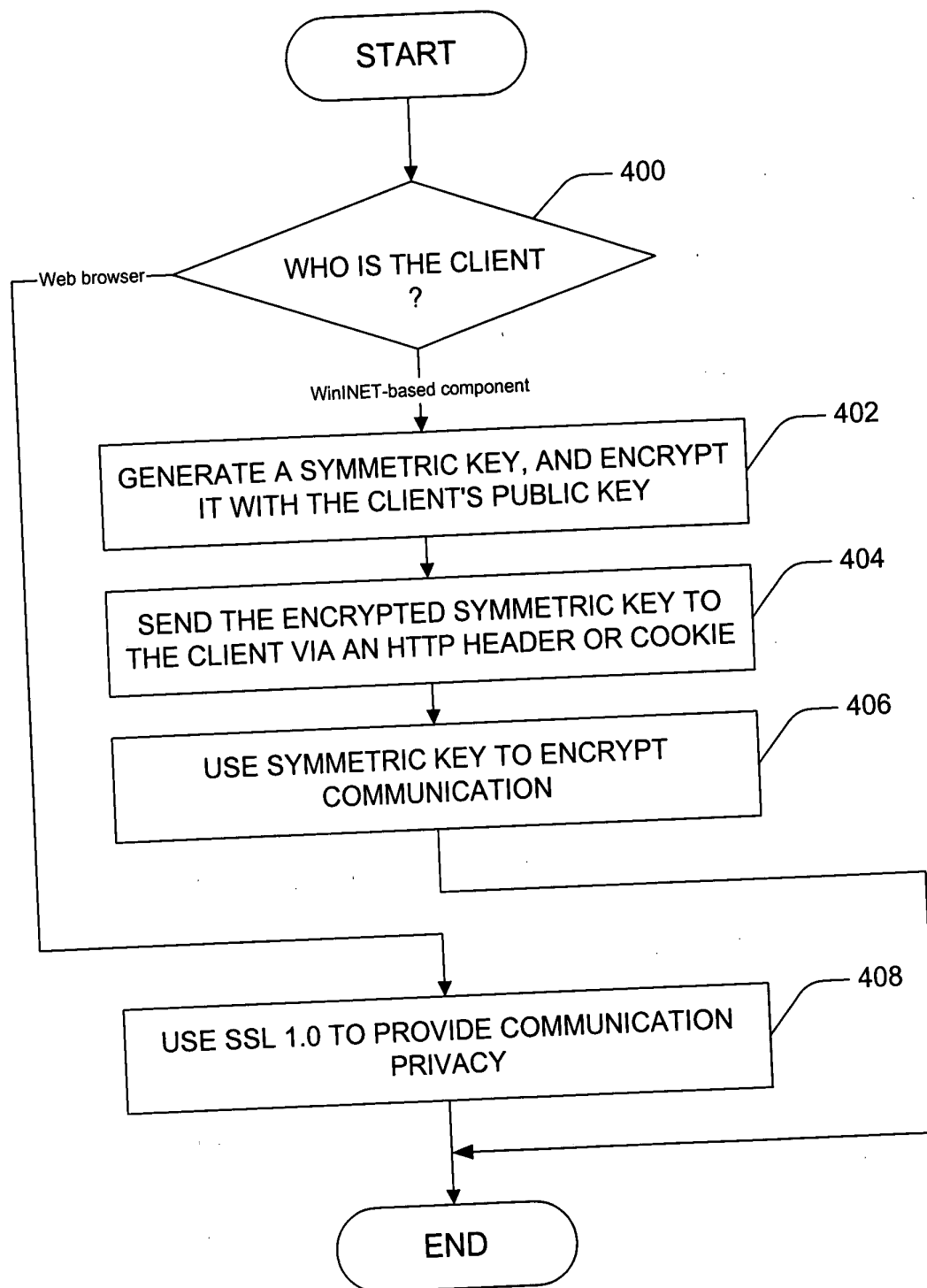


FIG. 4

PBCSA PROTOCOL FOR INITIAL HANDSHAKE

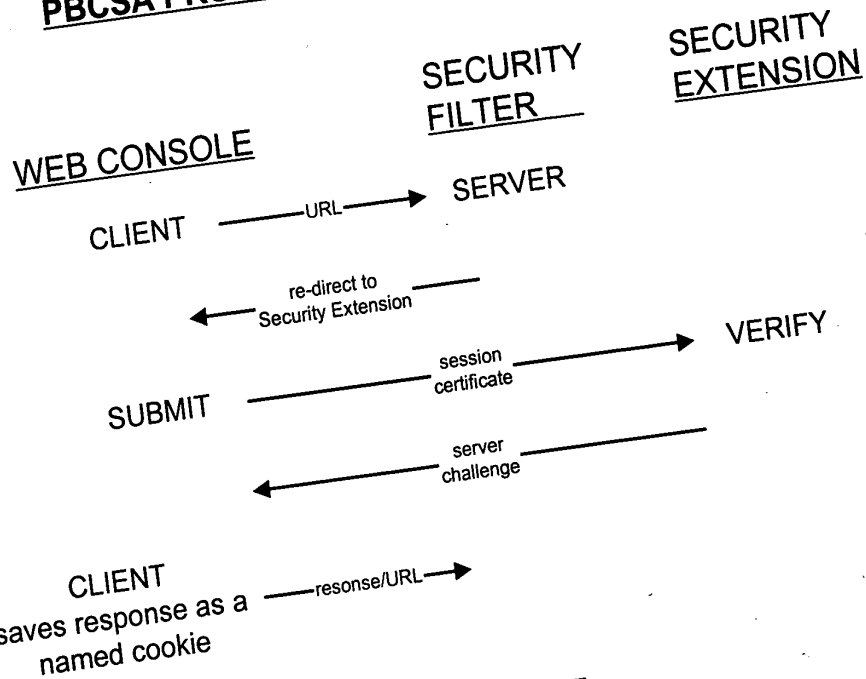


FIG. 5A

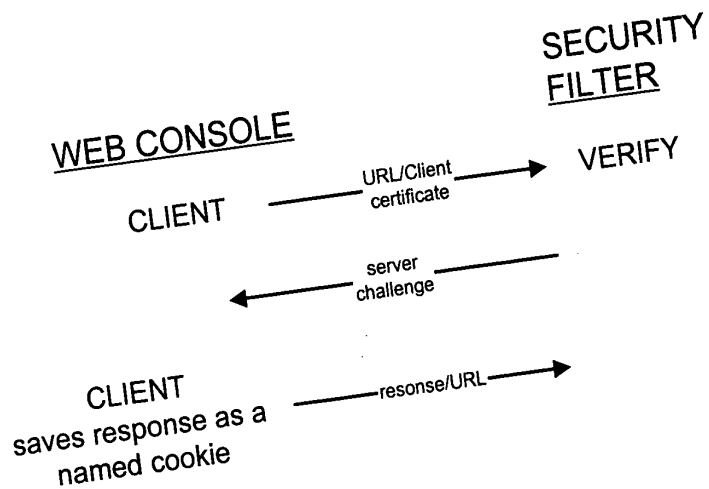


FIG. 5B

THE UNIVERSITY OF CHICAGO

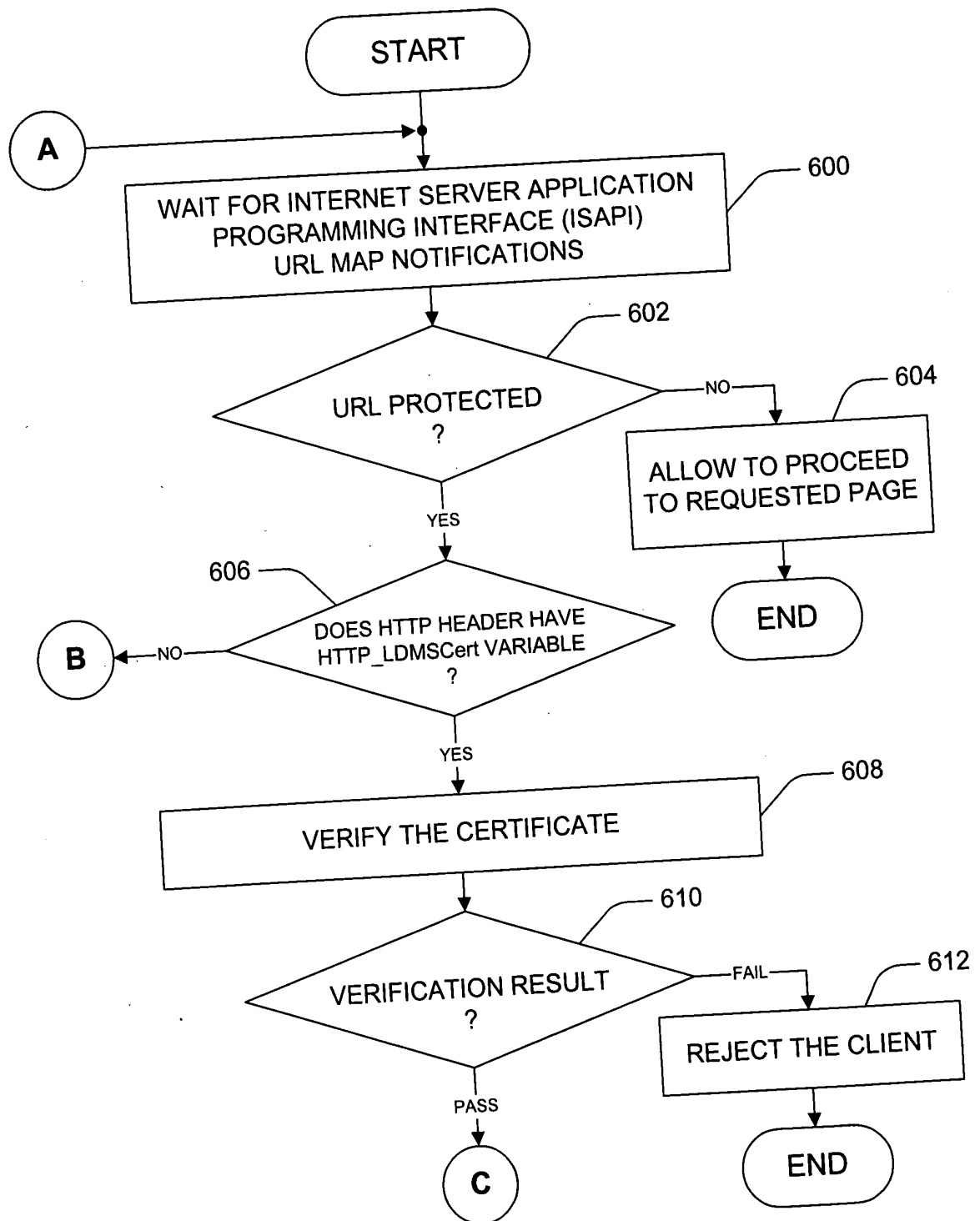


FIG. 6A

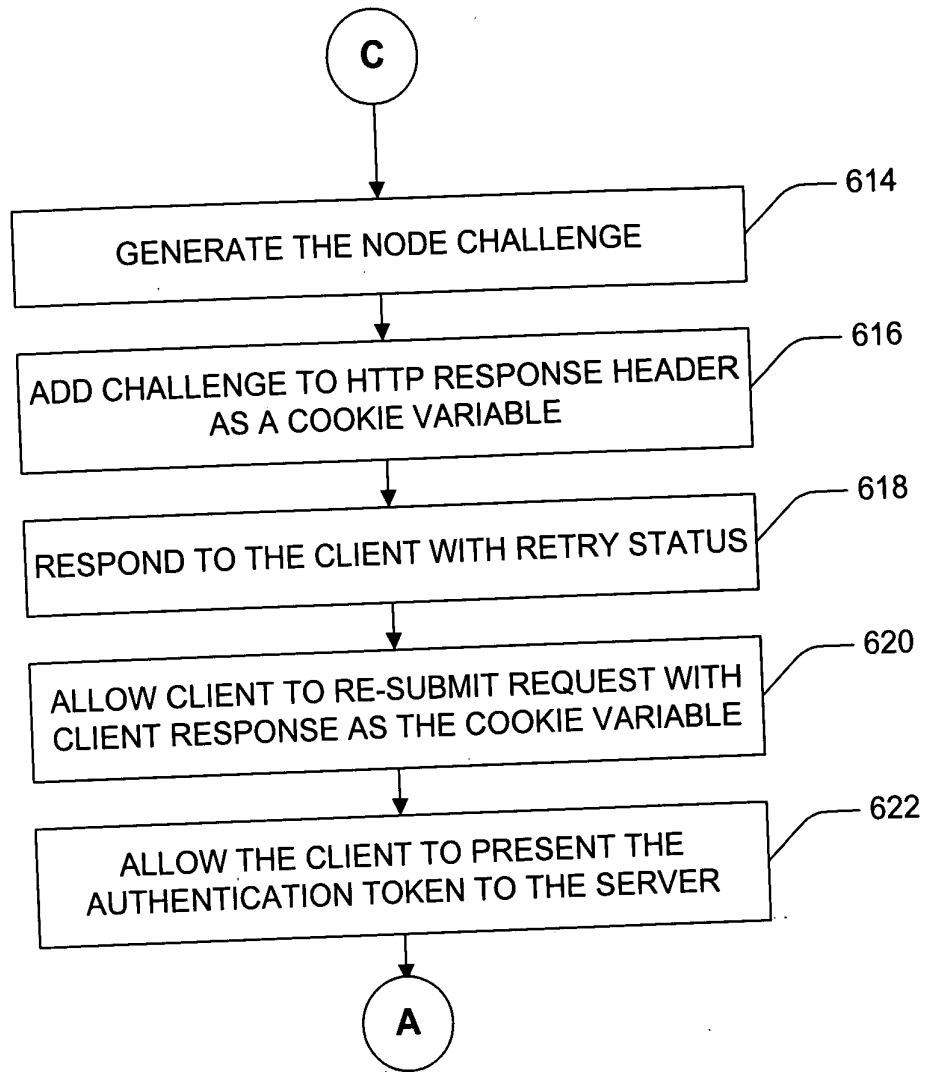


FIG. 6B

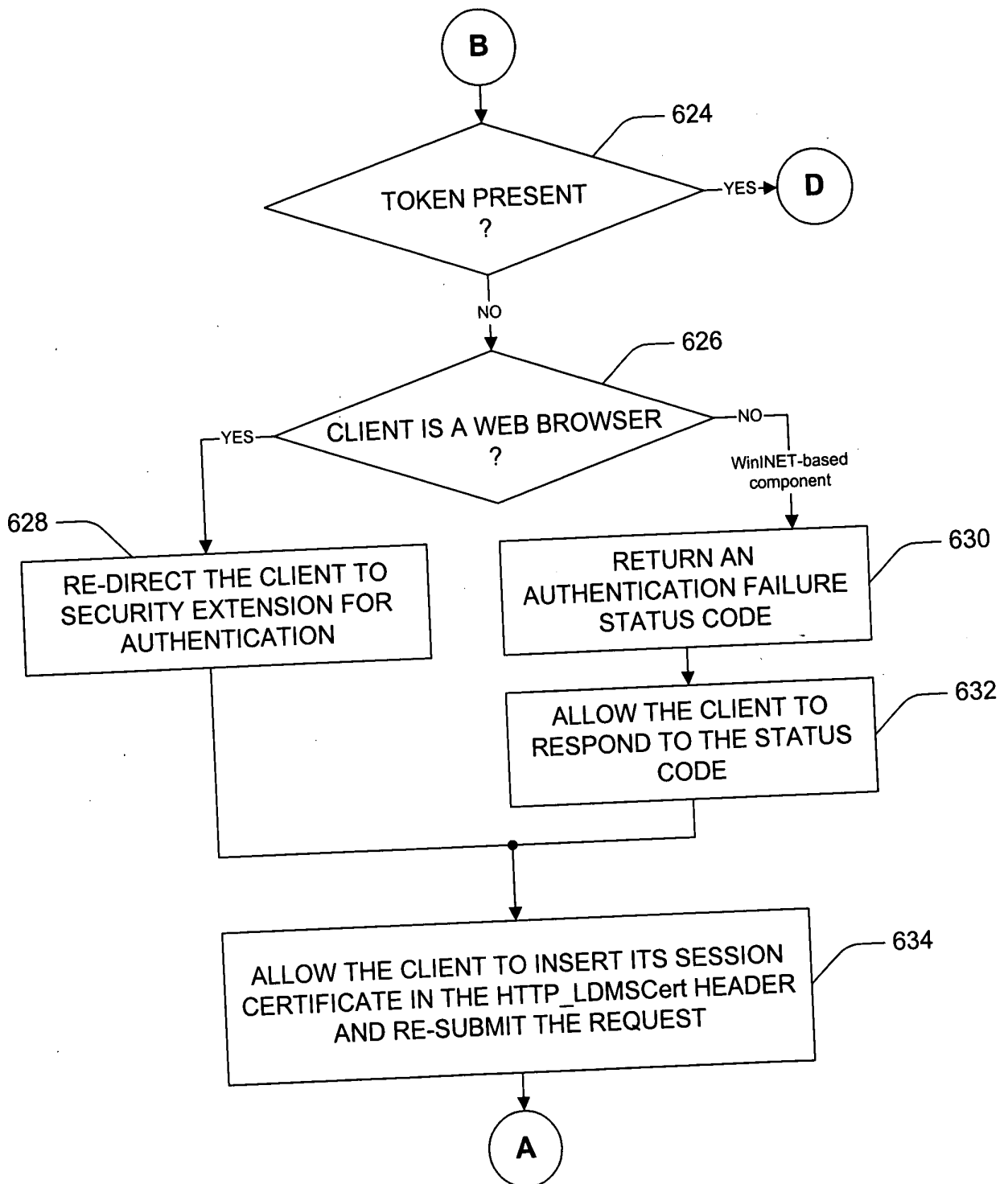


FIG. 6C

```

graph TD
    D((D)) --> 636{IS THE AUTHENTICATION TOKEN OF THE CLIENT RESPONSE VALID ?}
    636 -- NO --> 638[REJECT THE CLIENT]
    638 --> END1((END))
    636 -- YES --> 640{TOKEN EXPIRED ?}
    640 -- NO --> E((E))
    640 -- YES --> 642{CLIENT IS A WEB BROWSER ?}
    642 -- YES --> 644[RE-DIRECT THE CLIENT TO SECURITY EXTENSION]
    642 -- NO --> 646[RESPOND TO CLIENT WITH FAILURE STATUS]
    646 --> 648[ALLOW THE CLIENT TO INSERT A SESSION CERTIFICATE AS HTTP_LDMSCert VARIABLE]
    648 --> 650[RE-SUBMIT THE REQUEST TO THE MANAGED NODE]
    644 --> A((A))
    650 --> A

```

FIG. 6D

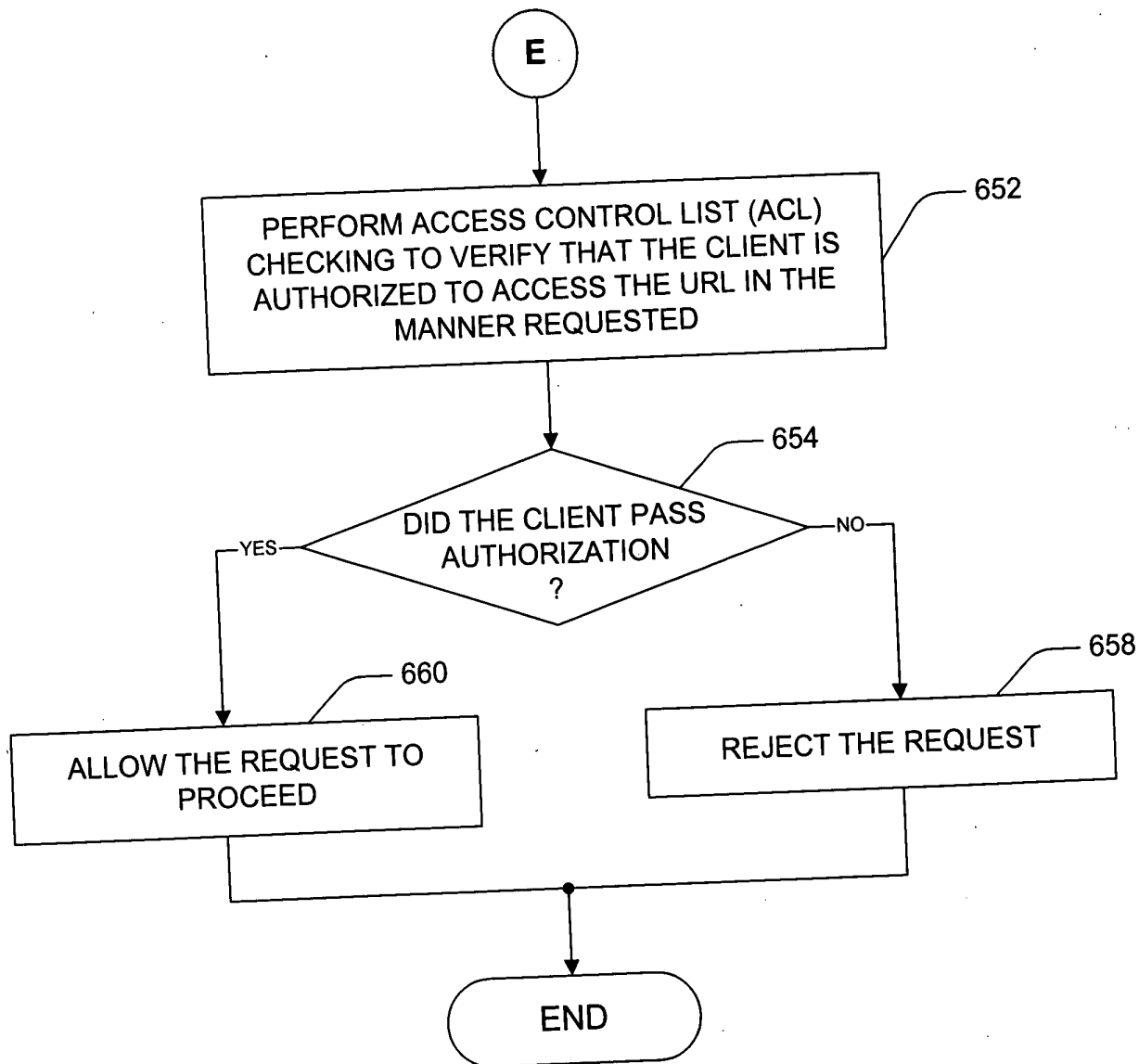


FIG. 6E

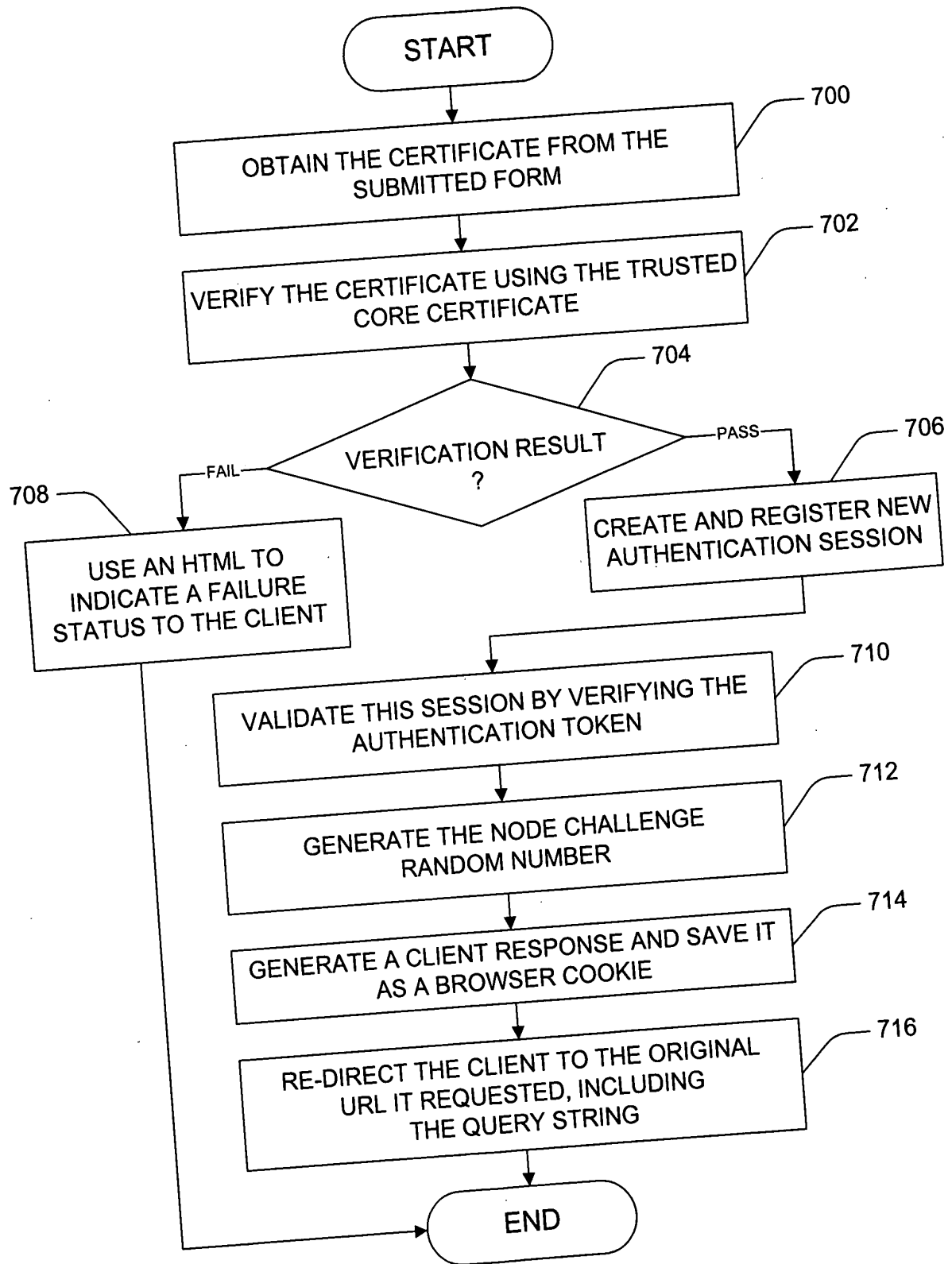


FIG. 7